Claims

1. A method for making a blind digital RSA-signature, comprising steps of: choosing secret factors and an RSA-module corresponding to them, choosing at least one admissible public RSA-exponent, choosing initial data, choosing a randomized blinding key, choosing an encryption RSA-key whose module corresponds to the chosen RSA-module and whose exponent corresponds to the chosen blinding key with which key an RSA-encryption is performed while creating blinded data, arbitrarily choosing a secret RSA-key corresponding to the chosen secret factors and an arbitrary admissible public RSA-exponent, and creating a digital RSA-signature on the blinded data corresponding to said secret RSA-key, unblinding the created digital RSA-signature on the blinded data by inputting the digital RSA-signature on the blinded data, the blinding key, the RSA module, and the public RSA-exponent corresponding to the secret RSA-key used in creating the digital RSA-signature on the blinded data, into an unblinding converter whose output data are obtained as the digital RSA-signature on the chosen initial data, *characterized* in that during the step of creating the blinded data an RSA-encryption of the chosen initial data is performed, during the step of unblinding the created digital RSA-signature on the blinded data the chosen initial data are input additionally into the unblinding converter, a masking factor coprime to each admissible public RSA-exponent is additionally chosen, and the blinding key is chosen coprime to each admissible public RSA-exponent and as a multiple to the chosen masking factor.

2. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that during the step of unblinding the created digital RSA-signature on the blinded data the chosen initial data preliminarily input into the unblinding converter are fed to one of base inputs of a modular multiplicative Euclidean converter (MMEC) contained in said unblinding converter, the created digital RSA-signature on the blinded data preliminarily input into the unblinding converter is fed to another base input of said unblinding converter, the chosen blinding key is fed to an exponent input of the MMEC corresponding to that base input on which said chosen initial data are fed, and the public RSA-exponent, which is preliminarily input into said unblinding converter and corresponds to the secret key utilized during creating the digital RSA-signature on the blinded data, is fed to an exponent input of the MMEC corresponding to that base input on which the created digital RSA-signature on the blinded data is fed.

3. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that the randomized blinding key is chosen by a random-number generator.

4. The method for making a blind digital RSA-signature according to Claim 3, *characterized* in that the step of choosing the randomized blinding key coprime to the chosen admissible public RSA-exponents is performed by correcting output data of the random-number generator with the chosen admissible public RSA-exponents.

5. The method for making a blind digital RSA-signature according to Claim 3, *characterized* in that the step of choosing the randomized blinding key is performed by testing whether the output data of the random-number generator are coprime to the chosen admissible public RSA-exponents.

6. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that the masking factor is chosen multiple to the greatest common divisor of the

secret factors decremented by 1, and also to each divisor which is less than the predetermined bound and modulo which at least one of the secret factors is congruent to 1.

7. The method for making a blind digital RSA-signature according to Claim 6, *characterized* in that the step of choosing the masking factor multiple to the greatest common divisor of the secret factors decremented by 1 is performed by choosing an RSA-module corresponding to two secret factors, and by choosing the masking factor multiple to the greatest one of those divisors of the RSA-module decremented by 1 that are coprime to the chosen admissible public RSA-exponents.

8. The method for making a blind digital RSA-signature according to Claim 7, *characterized* in that the step of choosing the masking factor multiple to the greatest one of those divisors of the RSA-module decremented by 1 that are coprime to the chosen admissible public RSA-exponents, is performed by choosing admissible public RSA-exponents coprime to said RSA-module decremented by 1, and by choosing said RSA-module decremented by 1 as the masking factor.

9. The method for making a blind digital RSA-signature according to Claim 6, *characterized* in that the step of choosing the masking factor multiple to each divisor which is less than the predetermined bound and modulo which at least one of the secret factors is congruent to 1, is performed by additionally testing the secret factors to be congruent to 1 modulo all those divisors which are greater than two and less than the predetermined bound.

10. The method for making a blind digital RSA-signature according to Claim 6, *characterized* in that the step of choosing the masking factor multiple to the greatest common divisor of the secret factors decremented by 1 is performed by additionally pairwise testing the secret factors, during the step of choosing them, for a simultaneous congruence to 1 modulo all those divisors that are greater than two, and by choosing the masking factor even, wherein in the step of choosing the secret factors a simultaneous pairwise non-congruence to 1 modulo all those divisors greater than two is accepted as a criterion of the step of choosing the secret factors.

11. The method for making a blind digital RSA-signature according to Claim 10, *characterized* in that the step of additionally pairwise testing the secret factors for a simultaneous congruence to 1 modulo all those divisors greater than two, is performed by comparing the value of the greatest common divisor of the secret factors decremented by 1 with an integer equal to two.

12. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that in the step of creating the blinded data the RSA-encryption of the chosen initial data is performed by means of a modular exponentiator.

13. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that an integer equal to two is chosen as the masking factor, during the step of choosing the secret factors they are additionally tested for a congruence to 1 modulo all those divisors greater than two and less than the predetermined bound and, pairwise, for a simultaneous congruence to 1 modulo all those divisors greater than two, wherein a non-congruence to 1 modulo all those divisors greater than two and less than the predetermined bound and a simultaneous pairwise non-congruence to 1 modulo all those divisors greater than two is accepted as a criterion of the step of choosing the secret factors.

14. The method for making a blind digital RSA-signature according to Claim 13, *characterized* in that in the step of choosing the secret factors, the step of additionally pairwise testing the secret factors for the simultaneous congruence to 1 modulo all those divisors greater than two is performed by comparing the value of the greatest common divisor of the secret factors decremented by 1 with an integer equal to two.

15. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that the RSA-signature on the blinded data is created by means of a modular exponentiator.

16. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that the RSA-module is chosen corresponding to two secret factors, the admissible public RSA-exponents are chosen coprime to the RSA-module decremented by 1, in the step of choosing the secret factors said secret factors are testing for a congruence to 1 modulo all those divisors greater than two and less than the predetermined bound, wherein a non-congruence to 1 modulo all those divisors greater than two and less than the predetermined bound is accepted as a criterion of the step of choosing the secret factors, and the masking factor is chosen multiple to the RSA-module decremented by 1.

17. The method for making a blind digital RSA-signature according to Claim 16, *characterized* in that the RSA-module decremented by 1 is chosen as the masking factor.

18. The method for making a blind digital RSA-signature according to Claim 6, or the Claim 13, or the Claim 16, *characterized* in that the predetermined bound is chosen according to the predetermined blinding level.

19. The method for making a blind digital RSA-signature according to Claim 1, *characterized* in that in the step of choosing the admissible public RSA-exponents an arbitrary public RSA-exponent whose only divisors are divisors of arbitrarily chosen basic public RSA-exponents is accepted as the admissible public RSA-exponent.

20. The method for making a blind digital RSA-signature according to Claim 19, *characterized* in that the step of choosing the blinding key coprime to each admissible public RSA-exponent is performed by testing whether said blinding key is coprime to each basic public RSA-exponent.

21. The method for making a blind digital RSA-signature according to Claim 19, *characterized* in that the step of choosing the blinding key coprime to each admissible public RSA-exponent is performed by correcting the output data of the random-number generator by the chosen basic public RSA-exponents.

22. A method for making a blind digital RSA-signature, comprising steps of: choosing secret factors and an RSA-module corresponding to them, choosing at least one admissible public RSA-exponent, choosing initial data, choosing a randomized blinding key, choosing an encryption RSA-key whose module corresponds to the chosen RSA-module and with which the RSA-encryption is performed while creating the blinded data, the chosen initial data being processed with a result of the RSA-encryption while creating the blinded data, arbitrarily choosing a secret RSA-key corresponding to the chosen secret factors and an arbitrary admissible public RSA-exponent, and creating a digital RSA-signature on the blinded data, corresponding to said secret RSA-key, creating an unblinding key corresponding to the blinding key and the secret RSA-key utilized while creating the digital RSA-signature on the blinded data, unblinding the created digital RSA-signature on the blinded data by inputting the digital RSA-signature on the blinded data, which step of unblinding is performed by inputting said digital RSA-signature, the unblinding key and the RSA-module into an unblinding converter whose output data are received as the digital RSA-signature on the chosen initial data, *characterized* in that during the step of choosing at least one admissible public RSA-exponent a step of additionally choosing at least one basic public RSA-exponent is performed, for each of which basic public RSA-exponents an arbitrary limiting multiplicity is chosen, and an arbitrary public RSA-exponent constituted from the chosen basic public RSA-exponents is accepted as the admissible public RSA-exponent, a multiplicity of each chosen basic public RSA-exponent being taken within a range of the chosen limiting multiplicity, during the step of creating the blinded data a step of RSA-encryption the chosen blinding key is performed, the encryption RSA-key by which the step of RSA-encryption being performed during the step of creating the blinded data is chosen corresponding to an RSA-exponent constituted from the chosen basic public RSA-exponents each of which being taken in the chosen limiting multiplicity, the step of arbitrarily choosing the secret RSA-key corresponding to the chosen secret factors and arbitrary admissible public RSA-exponent is performed by arbitrarily choosing utilized multiplicities of the basic public RSA-exponents within a range of the chosen limiting multiplicities of the basic public RSA-exponents, and the unblinding key is created by RSA-encryption of the blinding key with the encryption RSA-key as a module of which the RSA-module is taken, and whose RSA-exponent corresponds to the basic public RSA-exponents, each of said basic public RSA-exponents being taken in a multiplicity equal to the difference between the limiting multiplicity corresponding to said basic public RSA-exponent and the utilized multiplicity chosen in the step of arbitrarily choosing the secret key and corresponding to said limiting multiplicity.

23. The method for making a blind digital RSA-signature according to Claim 22, *characterized* in that the step of choosing the randomized blinding key is performed by means of a random-number generator.

24. The method for making a blind digital RSA-signature according to Claim 22, *characterized* in that in the step of creating the blinded data the step of RSA-encryption of the chosen blinding key is performed by consecutive RSA-encryptions with the encryption RSA-keys, the RSA-module being taken as a module of each of said RSA-keys, and the basic public RSA-exponents being taken as the RSA-exponents, each of said basic public RSA-exponents being taken in the chosen limiting multiplicity.

25. The method for making a blind digital RSA-signature according to Claim 22, *characterized* in that the step of creating the unblinding key by RSA-encryption of the blinding key with the encryption RSA-key is performed by consecutive RSA-encryptions with the encryption RSA-keys, the RSA-module being taken as a module of each of said RSA-keys, and the basic public RSA-exponents being taken as the RSA-exponents, each of said basic public RSA-exponents being taken in the multiplicity equal to the difference between the limiting multiplicity corresponding to said basic public RSA-exponent, and a utilized multiplicity chosen in the step of arbitrarily choosing the secret key and corresponding to said limiting multiplicity.

26. The method for making a blind digital RSA-signature according to Claim 22, *characterized* in that the step of RSA-encryption during steps of creating the blinded data and creating the unblinding key is performed by means of a modular exponentiator.

27. The method for making a blind digital RSA-signature according to Claim 22, *characterized* in that the digital RSA-signature on the blinded data is created by means of a modular exponentiator.

28. An apparatus for making a blind digital RSA-signature, comprising a blinding key choice unit having a random-number generator and a blinding unit having a modular exponentiator whose module input being connected to a module input of the blinding unit and whose exponent input being connected to a blinding key input of the blinding unit, said blinding unit has an initial data input and one output being connected to a signature data input of a signature unit which has a secret key input and one output being connected to an unblinding data input of an unblinding unit which has a signature output, a module input, an exponent input and a blinding key input, *characterized* in that a base input of the modular exponentiator of the blinding unit is connected to the initial data input of the blinding unit, and the output of the modular exponentiator is connected to the output of the blinding unit, the unblinding unit has additionally an initial data input and comprises a modular multiplicative Euclidean converter (MMEC) having a module input, base inputs and exponent inputs corresponding to each of said base inputs, the module input of the unblinding unit being connected to the module input of the MMEC, the initial data input of the unblinding unit being connected to one of the base inputs of the MMEC, and an unblinding data input of the unblinding unit being connected to another base input of the MMEC, the blinding key input of the unblinding unit is connected to the exponent input of the MMEC which corresponds to the base input of the MMEC connected to the unblinding data input of the unblinding unit, and the exponent input of the unblinding unit is connected to the exponent input of the MMEC which corresponds to the base input of the MMEC connected to the initial data input of the unblinding unit, and the output of the unblinding unit is connected to the output of the MMEC, the blinding key choice unit comprises additionally an arithmetic controller with two limiting inputs which are accepted conditionally as first and second limiting inputs, the arithmetic controller being connected to the random-number generator, an output of the arithmetic controller is connected to the output of the blinding key choice unit, and the arithmetic controller is made so as to provide output data of the blinding key choice unit coprime to integers fed onto the first limiting input of the arithmetic controller, and to provide the divisibility of the output data of the blinding key choice unit with an integer fed onto the second limiting input of the arithmetic controller.

29. The apparatus for making a blind digital RSA-signature according to Claim 28, *characterized* in that the connection of the arithmetic controller to the random-number generator is performed by means of connecting the output of the random-number generator to the input accepted conditionally as test data input of the arithmetic controller, and coprimality of the output data of the blinding key choice unit to integers fed onto the first limiting input of the arithmetic controller and the divisibility of the output data of the blinding key choice unit with an integer fed onto the second limiting input of the arithmetic controller are provided by means of that the arithmetic controller comprises a multiplier and a coprimality tester, the first limiting input of the arithmetic controller being connected to an input of the coprimality tester, the test data input being connected to another input of the coprimality tester and to an argument input of the multiplier, an output of the coprimality tester being connected to a loading input of the multiplier, and the second limiting input of the arithmetic controller being connected to the argument input of the multiplier, whose output is connected to the output of the arithmetic controller.